



OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

INSPECTION REPORT

DOE-OIG-18-19

February 2018

**ALLEGED INFORMATION
TECHNOLOGY WEAKNESSES AND
INAPPROPRIATE SYSTEM ACCESS AT
THE OAK RIDGE NATIONAL
LABORATORY**



Department of Energy
Washington, DC 20585

February 15, 2018

MEMORANDUM FOR THE DIRECTOR OF THE OFFICE OF INFORMATION SYSTEMS,
OFFICE OF ENVIRONMENTAL MANAGEMENT

Michelle Anderson

FROM: Michelle L. Anderson
Deputy Inspector General
for Audits and Inspections
Office of Inspector General

SUBJECT: INFORMATION: Inspection Report on “Alleged Information
Technology Weaknesses and Inappropriate System Access at the Oak
Ridge National Laboratory”

BACKGROUND

The Department of Energy’s Oak Ridge Office of Environmental Management’s (Environmental Management) mission, in part, includes de-inventorying uranium-233 at the Oak Ridge National Laboratory’s Building 3019. Isotek Systems, LLC (Isotek), an Environmental Management contractor at Oak Ridge National Laboratory, is tasked with de-inventorying the materials. Isotek uses the Honeywell Vindicator Information System (Vindicator), a stand-alone Federal information system, to administer the intrusion detection system needed to assist with the physical protection of Building 3019. National Strategic Protective Services, LLC, another contractor at Oak Ridge National Laboratory, is responsible for monitoring the intrusion detection system alarms. Environmental Management provides support for the Isotek contract and the Oak Ridge Office provides support for the National Strategic Protective Services, LLC contract. In order to accomplish Environmental Management’s mission, Isotek and National Strategic Protective Services, LLC have certain personnel that participate in the Human Reliability Program (HRP), a security and safety reliability program designed to ensure that employees meet the highest standards of reliability and physical and mental suitability.

The Office of Inspector General received a complaint alleging that: (1) Isotek personnel misused a former Technical Security Administrator’s (Technical Administrator) login credentials; (2) the current Technical Administrator accessed Vindicator without being HRP-certified; and (3) a note was displayed on a computer workstation informing users not to log off of Vindicator. We initiated this inspection to determine the facts and circumstances surrounding the allegations.

RESULTS OF INSPECTION

We substantiated the allegations that Isotek personnel had misused a former Technical Administrator’s login credentials to access Vindicator and that the current Technical

Administrator had accessed Vindicator prior to being HRP-certified. We did not substantiate the allegation that a note informing users to not log off of Vindicator was displayed on a computer workstation. Although, we substantiated the first two allegations, we also found that Isotek had stopped using the former Technical Administrator's login credentials to access Vindicator and that the current Technical Administrator was not required to be HRP-certified per Title 10 Code of Federal Regulations Part 712, *Human Reliability Program*, before accessing Vindicator. As such, we did not make any recommendations regarding these issues.

Isotek misused a former Technical Administrator's login credentials when it continued to use the former Technical Administrator's credentials to access Vindicator after the former Technical Administrator departed. Isotek personnel told us that Honeywell Vindicator Technologies, the Vindicator developer, recommended that the former Technical Administrator's account not be deleted nor the password changed when he departed due to concerns that the system might not operate properly if these modifications were made. Concerning the current Technical Administrator's HRP certification, Isotek personnel informed us and we confirmed that the Technical Administrator was not required to be HRP-certified to access Vindicator per Title 10 Code of Federal Regulations Part 712. Finally, we interviewed various personnel involved with Vindicator, including National Strategic Protective Services, LLC Security Police Officers and Isotek personnel, who stated that there was not a note on a computer workstation informing users to "not log off," as alleged. In addition, we did not see the note when we conducted a tour of the workstation.

While conducting this allegation-based inspection, we identified opportunities for improvement related to the management and oversight of Vindicator. Specifically: (1) Isotek personnel were not retaining pertinent Vindicator audit data; (2) the current Isotek Technical Administrator, also a system administrator, was continuously logged in at a computer workstation for at least a month; (3) annual security control assessments were not being completed on Vindicator; and (4) the Environmental Management Authorizing Official was not notified of significant changes made to the Windows operating system and Vindicator.

Isotek was not retaining Vindicator audit data, as required, because the data was purged during a system upgrade. After the upgrade, Isotek told us the audit data recording tool was turned off to troubleshoot system communication failures and then the system was accidentally set to overwrite the audit data after the recorded data reached a specific storage limit. According to Isotek personnel, the Technical Administrator is required to log off the system after each use; however, we were informed that the Technical Administrator was continuously logged on for at least a month because the Technical Administrator forgot to log off after addressing a technical difficulty. We were unable to determine if anyone misused the current Technical Administrator's credential during this period due to the lack of audit data. We also found that only one annual security control assessment was completed on Vindicator during the 4-year period we reviewed. Finally, we found that Environmental Management's Authorizing Official, the only individual that can explicitly accept the risk of a significant change such as a system upgrade, was not notified before the changes were made. In this case, the Authorizing Official was not notified of the system upgrade, in part, because a Risk Executive, whose responsibilities include the sharing of risk-related information such as system upgrades, had not been designated by Environmental Management.

While Environmental Management and Isotek took several corrective actions during our review to address the issues we identified related to audit data and Vindicator access processes, we made additional recommendations aimed at improving the overall management and oversight of Vindicator.

MANAGEMENT REACTION

Management concurred with the report's recommendations and provided a path forward to address the issues identified in the report. Management stated that actions to designate a Risk Executive for the Vindicator System had already been taken. In addition, a corrective action plan and milestone date had been developed to ensure required assessments of the Vindicator security controls are performed. Management's completed and planned actions are responsive to our recommendations.

Management's formal comments are included in Appendix 3.

cc: Deputy Secretary
Chief of Staff
Under Secretary for Science
Principal Deputy Assistant Secretary for Environmental Management
Deputy Director for Field Operations, Office of Science

ALLEGED INFORMATION TECHNOLOGY WEAKNESSES AND INAPPROPRIATE SYSTEM ACCESS AT THE OAK RIDGE NATIONAL LABORATORY

TABLE OF CONTENTS

Inspection Report

Details of Finding 1

Recommendations 6

Management Response and Inspector Comments 7

Appendices

1. Objective, Scope and Methodology 8

2. Prior Reports 10

3. Management Comments 11

ALLEGED INFORMATION TECHNOLOGY WEAKNESSES AND INAPPROPRIATE SYSTEM ACCESS AT THE OAK RIDGE NATIONAL LABORATORY

DETAILS OF FINDING

The Department of Energy's Oak Ridge Office of Environmental Management (Environmental Management) is responsible for the safe cleanup of environmental legacy, which includes de-inventorying uranium-233 at the Oak Ridge National Laboratory's Building 3019. Isotek Systems, LLC (Isotek), an Environmental Management contractor at Oak Ridge National Laboratory, is tasked with de-inventorying the materials. Isotek uses the Honeywell Vindicator Information System (Vindicator), a stand-alone Federal information system, to administer the intrusion detection system needed to assist with the physical protection of Building 3019. National Strategic Protective Services, LLC (NSPS), another contractor at Oak Ridge National Laboratory, is responsible for providing Central Alarm Station Operators and Security Police Officers to monitor intrusion detection system alarms. Environmental Management provides support for the Isotek contract and the Oak Ridge Office provides support for the NSPS contract. In order to accomplish Environmental Management's mission, certain Isotek and NSPS personnel participate in the Human Reliability Program (HRP), a security and safety reliability program designed to ensure that employees meet the highest standards of reliability and physical and mental suitability.

Vindicator can be accessed through three computer workstations that are separately located at Oak Ridge National Laboratory. Security controls for Federal information systems like Vindicator are developed using the Risk Management Framework to address security-related risks that arise from the loss of confidentiality, integrity, or availability of information or information systems. Isotek's Honeywell Vindicator Information System Security Plan was created using security controls from at least the moderate risk baseline, which is included in the National Institute of Standards and Technology 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.

We received a complaint alleging that: (1) Isotek personnel misused a former Technical Security Administrator's (Technical Administrator) login credentials; (2) the current Technical Administrator accessed Vindicator without being HRP-certified; and (3) a note was displayed on a computer workstation informing users not to log off of Vindicator. We substantiated the allegation that Isotek personnel had misused a former Technical Administrator's login credentials to access Vindicator and that the current Technical Administrator accessed Vindicator prior to being HRP-certified. Isotek personnel acknowledged that they had previously used the former Technical Administrator's credentials, but discontinued this practice prior to our review. In addition, the officials stated that they had taken corrective action to by upgrading the Windows operating system and Vindicator. Further, Isotek personnel informed us and we confirmed that the current Technical Administrator's access did not violate Title 10 Code of Federal Regulations Part 712 requirements. We did not substantiate the allegation that a note informing users to not log off of Vindicator was displayed on a computer workstation. Although, we substantiated two of the three allegations, we found that corrective actions were taken prior to receiving the allegations and Title 10 Code of Federal Regulations Part 712 requirements were not violated. Therefore, we did not make any recommendations pertaining to the allegations.

While conducting this allegation-based inspection, we identified opportunities for improvement related to the management and oversight of Vindicator. Specifically: (1) Isotek personnel were not retaining pertinent Vindicator audit data; (2) the current Isotek Technical Administrator, also a system administrator, was continuously logged in at a computer workstation for at least a month; (3) annual security control assessments were not being completed on Vindicator; and (4) the Environmental Management Authorizing Official was not notified of significant changes made to the Windows operating system and Vindicator.

Misuse of Login Credentials

We substantiated the allegation that Isotek personnel had misused a former Technical Administrator's login credentials to access Vindicator. Isotek personnel had taken corrective action to address this issue prior to our review to improve access by upgrading the Windows operating system and Vindicator. Isotek personnel told us that Honeywell recommended that the former Technical Administrator's account not be deleted nor the password changed due to concerns that the system might not work properly if the modifications were completed. Therefore, Isotek personnel decided not to log off of the former Technical Administrator's account to ensure system access was not lost. Further, Isotek personnel stated that corrective actions to change the user name and password could not be completed until the Windows operating system and Vindicator were upgraded, or a new information system was purchased. Oak Ridge National Laboratory officials gave Isotek approval to upgrade Vindicator in August 2015, and Isotek personnel completed the upgrade on October 31, 2015. Isotek's Vindicator Information System Security Plan requires a separation of duties for the following positions: Information System Security Manager, Information System Security Officer, and System Administrator. During the former Technical Administrator's employment, Isotek personnel had not fully implemented the separation of duties security control. The former Technical Administrator was also a system administrator for Vindicator. After upgrading the operating system, Isotek personnel created three new system administrator accounts, thereby resolving the separation of duties requirement and discontinuing the use of the former Technical Administrator's login credentials.

Improper Access to Vindicator

We substantiated the allegation that the current Technical Administrator, who is also a system administrator for Vindicator, accessed Vindicator prior to receiving HRP certification; however, we were informed and confirmed that the Technical Administrator's access to Vindicator did not violate requirements from Title 10 Code of Federal Regulations Part 712. The current Technical Administrator was hired by Isotek on December 30, 2013, and received HRP certification 6 months later on June 5, 2014. We were told that HRP certification is required to enter the area where Vindicator is located and that HRP certification is not required for the current Technical Administrator to access Vindicator. In this case, Isotek personnel informed us that an HRP-certified individual escorted the current Technical Administrator each time the Technical Administrator entered the area where Vindicator is located and accessed the system. In addition, we were told by Isotek personnel that the current Technical Administrator was not assigned duties requiring HRP certification until he was HRP-certified.

Note Display

We did not substantiate that a note informing users not to log off of Vindicator was displayed on a computer workstation. However, as previously discussed, we confirmed that the former Technical Administrator's account was not logged off to ensure that system access was not lost. Our interviews of NSPS Security Police Officers and Isotek personnel (who were all users, user supervisors, or Vindicator application managers) revealed that none of the individuals saw a note on any of the computer workstations. We also did not see the note when we conducted a tour of the workstations.

Other Matters

While conducting this allegation-based inspection, we identified opportunities for improvement related to the management and oversight of Vindicator. Specifically: (1) Isotek personnel were not retaining pertinent Vindicator audit data; (2) the current Isotek Technical Administrator, also a system administrator, was continuously logged in at a computer workstation for at least a month; (3) annual security control assessments were not being completed on Vindicator; and (4) the Environmental Management Authorizing Official was not notified of significant changes made to the Windows operating system and Vindicator.

Audit Data

During our inspection, we determined that Isotek personnel were not capturing or retaining required audit data used to determine information such as who, when, and the duration of time individuals were logged into Vindicator. Isotek's Vindicator Information System Security Plan requires that audit data be retained for 1 year and contain all identifying information for specific audit events, which includes successful and unsuccessful logons and logoffs; system accesses by privileged users; and starting and ending times for each instance a user accessed the system. One of the primary complaints in the allegation was that Isotek personnel continued to use a former Technical Administrator's login credentials to remain logged into Vindicator. However, since we were unable to obtain historical audit data from Vindicator, we had to rely heavily upon verbal testimony to conduct our inspection of the allegation.

Further, contrary to the 1-year retention requirement, Isotek personnel informed us that all audit data prior to October 31, 2015, had been disposed of during the Vindicator upgrade, and that the upgraded system began capturing data on October 31, 2015. We were later informed that audit data from December 2015 through April 6, 2016, was not available because of two separate events.¹ First, Isotek personnel failed to turn the audit data recording tool back on after a troubleshooting event, and second, audit data was deleted due to the selection of an improper setting that deleted the data instead of archiving the data. As a result of these two events, Isotek personnel were unable to provide us with specific audit data for the period of October 31, 2015, through April 6, 2016. During our review, Isotek personnel took several corrective actions, which included: (1) activating the audit data recording tool, changing the audit setting to archive, performing a demonstration to show that the system was currently tracking and

¹ We did not include October 31, 2015, through December 2015, because Isotek could not provide dependable audit logs due to this being a trial period for the upgraded system.

archiving audit data, and providing documentation to show that current quarterly reviews indicate that audit data is being retained and available; and (2) referring the incident to Isotek's Incident of Security Concern Inquiry Official who determined the audit data recording issue was a low impact security finding that was addressed.

Computer Workstation Logon

We identified an instance in which the Vindicator access protocols were not being followed. Specifically, we were told that the current Technical Administrator, who is also a system administrator for Vindicator, was logged in at a computer workstation continuously for at least a month. According to Isotek personnel, the Technical Administrator is required to log off of the system after each use; however, we were informed that the Technical Administrator was continuously logged on for at least a month because the Technical Administrator forgot to log off after addressing a technical difficulty. Audit data was not available for us to verify the statement that the current Technical Administrator was logged on for at least a month or if anyone misused the current Technical Administrator's credential while he was logged on. Subsequently, we were also informed that NSPS Lieutenants, who are required to log on and log off of the computer workstation at the beginning and end of each shift, were not doing so. As a result of our review: (1) the current Technical Administrator immediately logged off of the system; (2) Isotek personnel promptly notified the Incident of Security Concern Inquiry Official, who conducted an assessment and determined the incident to be a low impact security finding that Isotek personnel had addressed; (3) NSPS issued a bulletin requiring the Lieutenants to log on and log off at the beginning and end of the respective shifts; (4) Isotek's Information System Security Officer implemented a security measure to automatically log system administrators off of Vindicator workstations after 15 minutes of inactivity; and (5) Isotek personnel informed us and provided documentation to show that Isotek personnel were monitoring the log on and log offs during the quarterly reviews.

Security Control Assessments

We found that annual security control assessments of Vindicator were completed only once during a 4-year period. Isotek's Vindicator Information System Security Plan requires that the system be inspected annually. We requested the annual security control assessments performed on Vindicator. We were provided with an applicable assessment, a 2013 assessment, and told that annual assessments were not conducted during fiscal years 2014, 2015, and 2016. In November 2014, Environmental Management's Office of Corporate Information Technology^{2/} conducted an initial discovery to begin incorporating Isotek into its cybersecurity program, and in 2016, performed a site visit to assist Isotek personnel in the transition to the current cybersecurity requirements contained in Department Order 205.1b, Change 3, *Department of Energy Cyber Security Program*. Because of this transition to the current Department Order, the annual security control assessments were not performed. According to Office of Corporate Information Technology officials, once this transition is complete, the office will start performing the annual security control assessments.

² The Office of Environmental Management's Office of Corporate Information Technology changed its name to Office of Information Systems on November 10, 2016.

Additionally, Isotek personnel informed us that they had not always conducted quarterly reviews of the audit data, as required. However, during our review Isotek personnel informed us and provided documentation to show that quarterly audit log reviews were being completed as of May 2016. We were told that the reviews included assessments of user log on and log offs and to date had not identified any issues in these areas. Additionally, Isotek personnel performed a demonstration to show us that audit data was now being extracted from the system and retained in a separate database.

Significant Changes

We also found that Environmental Management's Authorizing Official was not notified of significant changes to the Windows operating system and Vindicator before they were made on October 31, 2015. Per National Institute of Standards and Technology Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Environmental Management's Risk Executive should notify the Authorizing Official of any change that is likely to affect the security state of an information system that includes, among other examples, installation of a new or upgraded operating system. The National Institute of Standards and Technology Special Publication also states that an Authorizing Official is the only individual that can explicitly accept the risk and authorize the use of a Federal information system. In this case, the Environmental Management Authorizing Official was not notified of the system upgrade, in part, because a Risk Executive, whose responsibilities include the sharing of risk-related information such as system upgrades, had not been designated. As a result, the Environmental Management Authorizing Official's duty to make potential risk-based decisions was limited when not made aware of the system changes. Subsequently, on February 5, 2016, the Authorizing Official appointed an Authorizing Official Designated Representative. The Authorizing Official Designated Representative was delegated the authority to act on behalf of the Authorizing Official in matters pertaining to the security of information technology systems and was tasked to keep the Authorizing Official informed of significant security related changes to systems and associated risks. However, at the time of our inspection, a Risk Executive, who is responsible for keeping the Authorizing Official Designated Representative apprised of significant security related changes to systems and associated risks, had not been appointed.

RECOMMENDATIONS

To address the issues identified in this report, we recommend Environmental Management's Director of the Office of Information Systems:

1. Ensure required assessments of the Vindicator security controls are performed; and
2. Designate a Risk Executive for the Vindicator System to ensure that the Authorizing Official is notified of significant changes made to Vindicator.

MANAGEMENT RESPONSE

In its response provided to the Office of Inspector General on November 6, 2017, management agreed with our findings and recommendations and provided corrective actions that were either completed or were planned to address our recommendations. On October 19, 2017, management designated a Risk Executive for the Vindicator System to ensure that the Authorizing Official is notified of significant changes made to Vindicator. Management advised that they have developed a corrective action plan and milestone date to implement the recommendation to ensure required assessments of the Vindicator security controls are performed.

INSPECTOR COMMENTS

The Department's completed and planned actions are responsive to our findings and recommendations. In a subsequent communication, the Department revised the estimated completion date for the remaining action to March 2018. Management's comments and corrective actions are included in Appendix 3.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The Office of Inspector General received a complaint alleging that: (1) Isotek Systems, LLC personnel misused a former Technical Security Administrator's login credentials; (2) the current Technical Security Administrator improperly accessed the Honeywell Vindicator Information System without being Human Reliability Program-certified; and (3) a note was displayed on a computer workstation informing users not to log off of the Honeywell Vindicator Information System. We initiated this inspection to determine the facts and circumstances surrounding the allegations.

Scope

We conducted this inspection from March 2016 through February 2018 at the Department of Energy's Oak Ridge National Laboratory and Office of Environmental Management located in Oak Ridge, Tennessee. The inspection was conducted under the Office of Inspector General project code S16IS005.

Methodology

To accomplish the inspection objective, we:

- Performed facility walkthroughs of the Honeywell Vindicator Information System computer workstation locations at Oak Ridge National Laboratory to gain an understanding of the facilities and to determine if the note mentioned in the allegation was present;
- Obtained and reviewed the applicable Federal regulations, and Department and contractor policies pertaining to Federal information systems and the Human Reliability Program;
- Obtained and reviewed Honeywell Vindicator Information System's Security and Contingency Plans, Honeywell Vindicator Information System's Risk Assessment, Office of Environmental Management's Risk Management Approach Implementation Plan, Isotek Systems, LLC's and National Strategic Protective Service's Human Reliability Implementation Plans, and Isotek Systems, LLC's Firm Fixed-Price Contract;
- Obtained and reviewed prior Office of Inspector General reports and Federal Oversight reports;
- Conducted interviews of Department, National Strategic Protective Services, Oak Ridge Office, and Isotek Systems, LLC personnel; and
- Requested audit logs from January 2013 through February 2016.

We conducted this allegation-based inspection in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*, dated January 2012. Those standards require that we plan and perform the inspection to obtain sufficient, appropriate evidence to provide a reasonable basis for our conclusions and observations based on our inspection objective. We believe the evidence obtained provided a reasonable basis for our conclusions and observations based on our inspection objective. Accordingly, the inspection included tests of controls and compliance with laws and regulations to the extent necessary to satisfy the inspection objective. Because our review was limited, it may not necessarily have disclosed all internal control deficiencies that may have existed at the time of our inspection. Also, we assessed the Department's compliance with the *Government Performance and Results Modernization Act of 2010* and identified cybersecurity performance measures. Finally, we did not rely on computer-processed data relevant to our inspection objective due to pertinent audit data not being available during the scope of our review.

Management waived an exit conference on November 21, 2017.

PRIOR REPORTS

- Evaluation Report on [*The Department of Energy's Unclassified Cybersecurity Program - 2015*](#) (DOE-OIG-16-01, November 2015). The review was a follow-up of 26 previously identified cybersecurity weaknesses related to its unclassified cybersecurity program. The review noted that the Department of Energy made significant progress in remediating weaknesses identified in a fiscal year 2014 evaluation, which resulted in the closure of 22 of 26 reported deficiencies. However, the current review identified issues related to security reporting, vulnerability management, system integrity of Web applications, and account management. The weaknesses identified occurred, in part, because the Department had not ensured that policies and procedures were fully developed and/or implemented to meet all necessary cybersecurity requirements.
- Audit Report on [*Cybersecurity Controls Over a Major National Nuclear Security Administration Information System*](#) (DOE/IG-0938, June 2015). The review found that the system's cybersecurity controls had not been adequately developed, documented, or implemented. Specifically, user passwords had not been regularly changed to reduce the risk of system compromise and ensure that users had been authorized to maintain access to the system. Additionally, controls over database change management had not been fully developed or implemented. Specifically, separation of duties and role-based access controls had not been fully implemented. The weaknesses identified occurred, at least in part, because site officials did not ensure that Federal security requirements were fully implemented to protect the system.

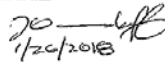
MANAGEMENT COMMENTS



Department of Energy
Washington, DC 20585

JAN 26 2018

MEMORANDUM FOR APRIL G. STEPHENSON
ACTING INSPECTOR GENERAL

FROM: JAMES M. OWENDOFF 
PRINCIPAL DEPUTY ASSISTANT SECRETARY
FOR ENVIRONMENTAL MANAGEMENT

SUBJECT: Inspector General Request for Office of Environmental Management
Review and Concurrence on the IG Draft Report *Alleged Information
Technology Weaknesses and Inappropriate System Access at the Oak
Ridge National Laboratory* (S16IS005)

The purpose of this memorandum is to provide you with the Office of Environmental Management (EM) concurrence on the Office of the Inspector General (IG) Draft Report *Alleged Information Technology Weaknesses and Inappropriate System Access at the Oak Ridge National Laboratory*, in response to the IG request of October 13, 2017.

We agree with the findings and recommendations. On October 19, 2017, we completed the recommendation to designate a Risk Executive for the Vindicator System to ensure that the Authorizing Official is notified of significant changes made to Vindicator. We have developed a corrective action plan and milestone date to implement the IG recommendation to ensure required assessments of the Vindicator security controls are performed (copy attached). We coordinated this draft report with the Oak Ridge Office and the Office of Science.

We will provide quarterly status updates on the remaining corrective action in the Departmental Audit Reporting and Tracking System.

Thank you for the opportunity to review and respond to this draft report.

If you have any questions, please contact me or Ms. Jeanne Beard, Director for Communications, at (202) 586-0200 or at jeanne.beard@em.doe.gov.

Attachment



CORRECTIVE ACTION PLAN
IG INSPECTION REPORT: Alleged Information Technology
Weaknesses and Inappropriate System Access at the Oak Ridge National Laboratory
S16IS005

Recommendation 1: Ensure required assessments of the Vindicator security controls are performed.

Corrective Action Plan: The EM Office of Information Systems, EM-5.12, will integrate the Isotek Vindicator System into the EM Information Security Continuous Monitoring (ISCM) Program. The EM ISCM program conducts annual assessments of EM site information systems to determine the site's compliance with DOE 205.1B and the EM *Risk Management Approach Implementation Plan*. Integration of the Vindicator system is planned for January 2018.

Recommendation 2: Designate a Risk Executive for the Vindicator System to ensure that the Authorizing Official is notified of significant changes made to Vindicator.

Corrective Action Plan: The Oak Ridge Environmental Management Office, at the direction of EM Office of Information Systems, EM-5.12, has appointed the Risk Executive function. The appointment of the Risk Executive occurred on October 19, 2017.

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions, and feedback to OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. Comments may also be mailed to:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at (202) 253-2162.